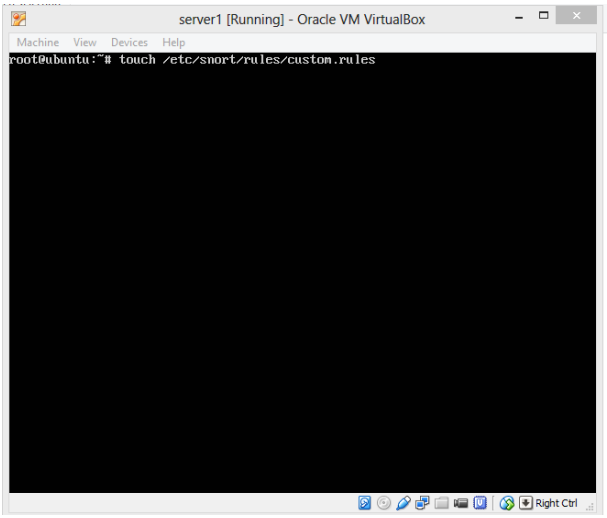
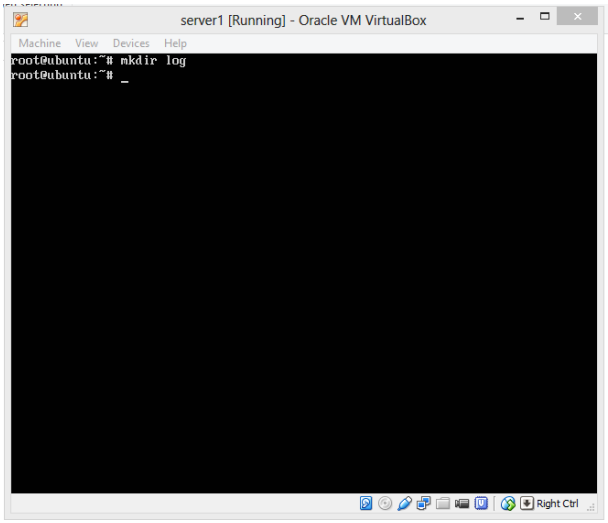
Keamanan Jaringan Komputer
Operasi Snort

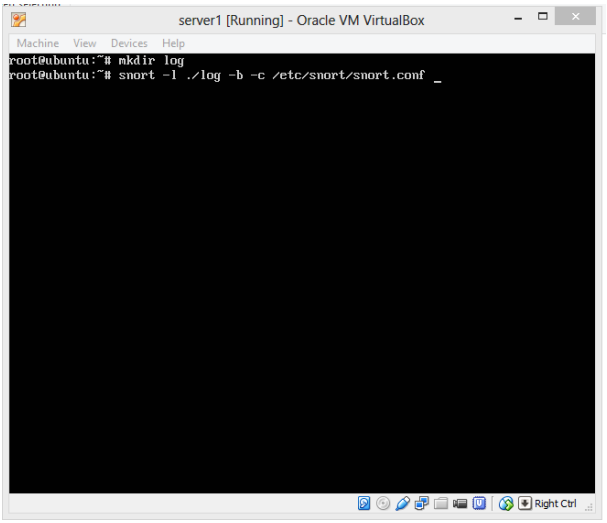
Disusun Oleh :
Nama : Imam Mustofa
NIM : 09011181320028

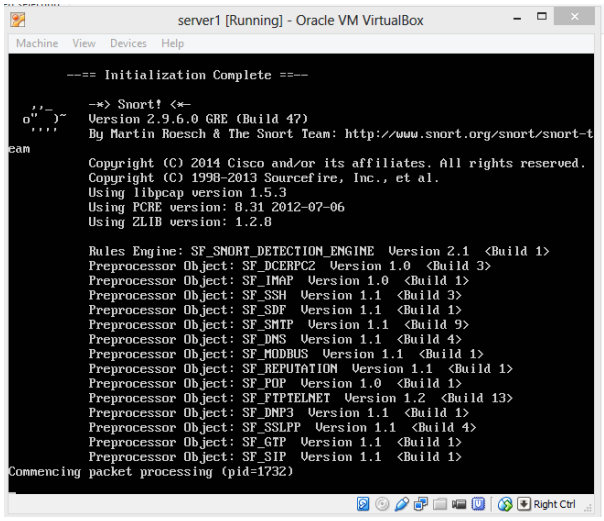
SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA
2017

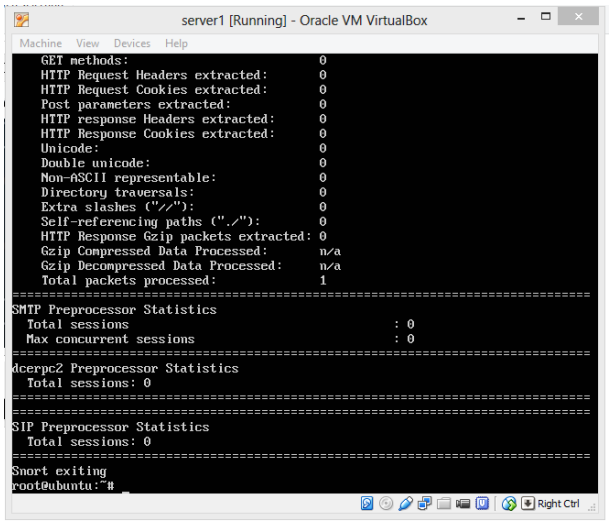
Berikut adalah uraian data penggunaan snort sebagai analisis alert terhadap penyerangan dalam jaringan

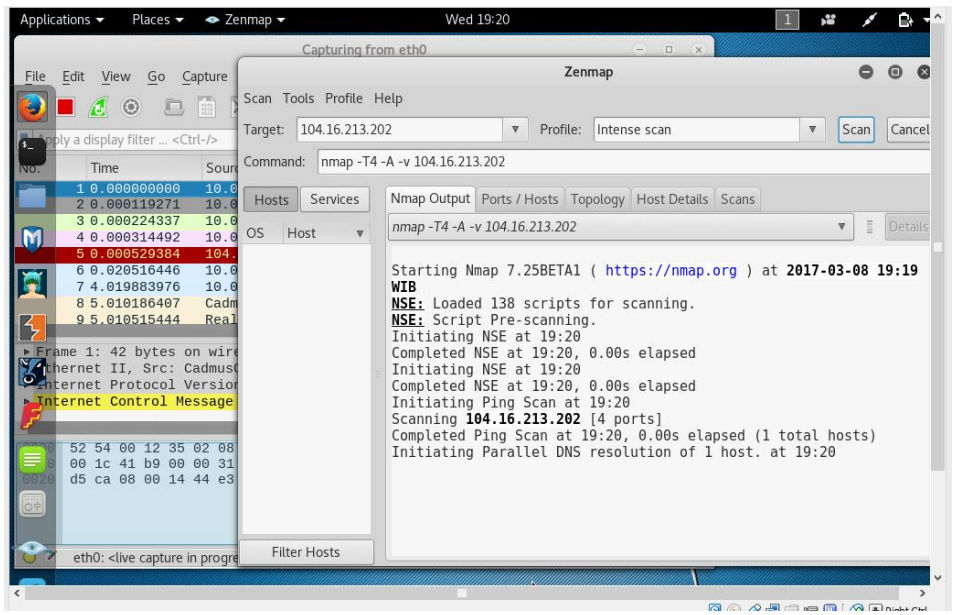


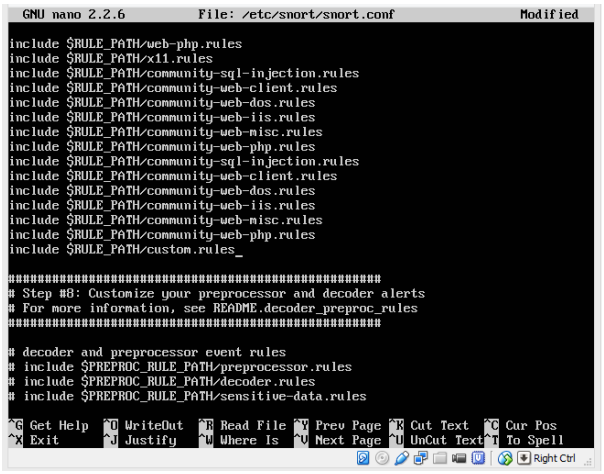


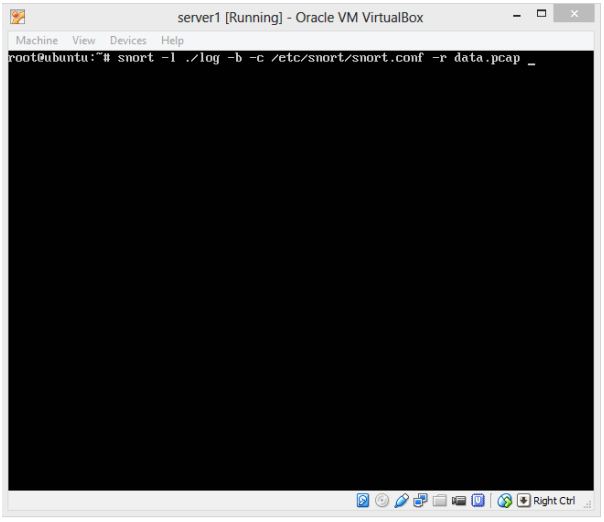


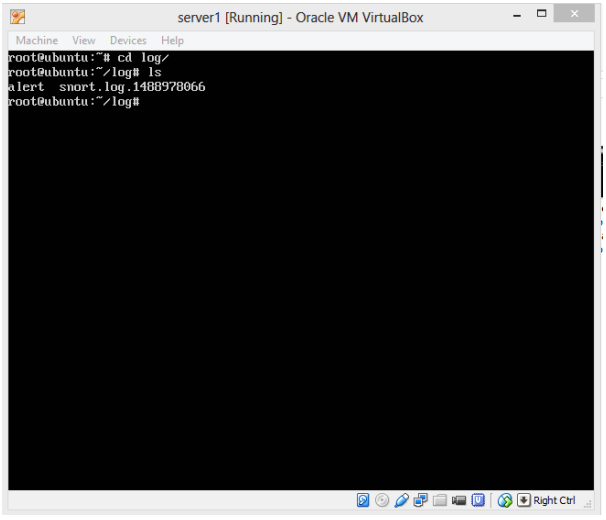

server1 [Running] - Oracle VM VirtualBox
Machine View Devices Help
--== Initialization Complete ==--
-*> Snort! <*-
Version 2.9.6.0 GRE (Build 47)
By Martin Roesch & The Snort Team: http://www.snort.org/snort/snort-team
Copyright (C) 2014 Cisco and/or its affiliates. All rights reserved.
Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using libpcap version 1.5.3
Using PCRE version: 8.31 2012-07-06
Using ZLIB version: 1.2.8
Rules Engine: SF_SNORT_DETECTION_ENGINE Version 2.1 <Build 1>
Preprocessor Object: SF_DCERPC2 Version 1.0 <Build 3>
Preprocessor Object: SF_IMAP Version 1.0 <Build 1>
Preprocessor Object: SF_SSH Version 1.1 <Build 3>
Preprocessor Object: SF_SDF Version 1.1 <Build 1>
Preprocessor Object: SF_SMTP Version 1.1 <Build 9>
Preprocessor Object: SF_DNS Version 1.1 <Build 4>
Preprocessor Object: SF_MODBUS Version 1.1 <Build 1>
Preprocessor Object: SF_REPUTATION Version 1.1 <Build 1>
Preprocessor Object: SF_POP Version 1.0 <Build 1>
Preprocessor Object: SF_FTPTELNET Version 1.2 <Build 13>
Preprocessor Object: SF_DNP3 Version 1.1 <Build 1>
Preprocessor Object: SF_SSLPP Version 1.1 <Build 4>
Preprocessor Object: SF_GTP Version 1.1 <Build 1>
Preprocessor Object: SF_SIP Version 1.1 <Build 1>
Commencing packet processing (pid=1732)
Right Ctrl

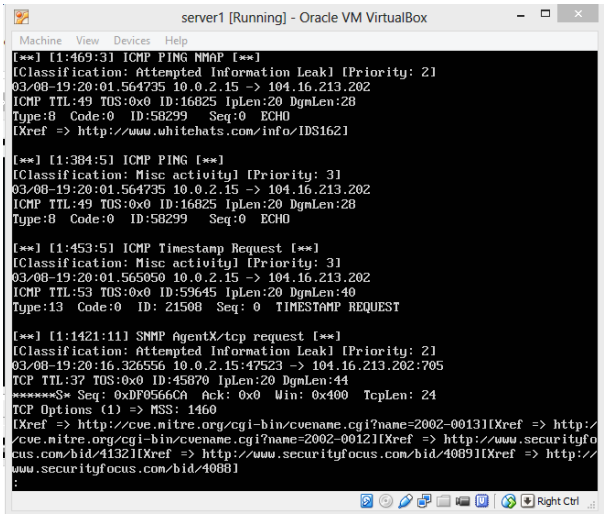

server1 [Running] - Oracle VM VirtualBox
Machine View Devices Help
GET methods: 0
HTTP Request Headers extracted: 0
HTTP Request Cookies extracted: 0
Post parameters extracted: 0
HTTP response Headers extracted: 0
HTTP Response Cookies extracted: 0
Unicode: 0
Double unicode: 0
Non-ASCII representable: 0
Directory traversals: 0
Extra slashes ("//"): 0
Self-referencing paths ("./"): 0
HTTP Response Gzip packets extracted: 0
Gzip Compressed Data Processed: n/a
Gzip Decompressed Data Processed: n/a
Total packets processed: 1
SMTP Preprocessor Statistics
Total sessions : 0
Max concurrent sessions : 0
dcerpc2 Preprocessor Statistics
Total sessions: 0
SIP Preprocessor Statistics
Total sessions: 0
Snort exiting
root@ubuntu:~#
Right Ctrl

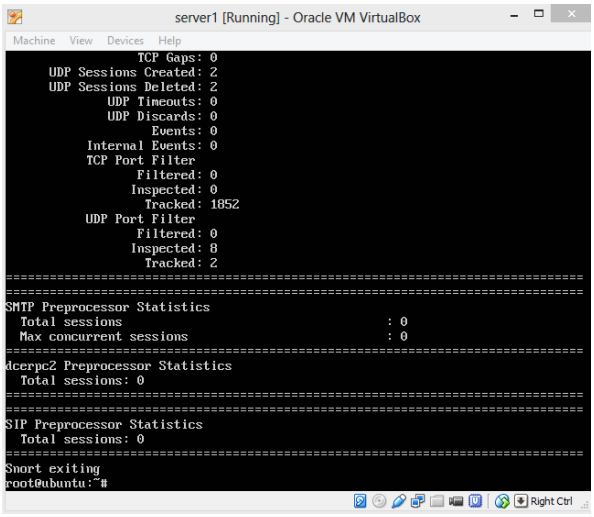

Applications Places Zenmap Wed 19:20
Capturing from eth0
File Edit View Go Capture
Zenmap
Scan Tools Profile Help
Target: 104.16.213.202
Profile: Intense scan
Scan Cancel
Command: nmap -T4 -A -v 104.16.213.202
Hosts Services
OS Host
Nmap Output Ports / Hosts Topology Host Details Scans
nmap -T4 -A -v 104.16.213.202
Details
Starting Nmap 7.25BETA1 (https://nmap.org) at 2017-03-08 19:19 WIB
NSE: Loaded 138 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 19:20
Completed NSE at 19:20, 0.00s elapsed
Initiating NSE at 19:20
Completed NSE at 19:20, 0.00s elapsed
Initiating Ping Scan at 19:20
Scanning 104.16.213.202 [4 ports]
Completed Ping Scan at 19:20, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 19:20
Filter Hosts


GNU nano 2.2.6 File: /etc/snort/snort.conf Modified
include $RULE_PATH/web-php.rules
include $RULE_PATH/x11.rules
include $RULE_PATH/community-sql-injection.rules
include $RULE_PATH/community-web-client.rules
include $RULE_PATH/community-web-dos.rules
include $RULE_PATH/community-web-iis.rules
include $RULE_PATH/community-web-misc.rules
include $RULE_PATH/community-web-php.rules
include $RULE_PATH/community-sql-injection.rules
include $RULE_PATH/community-web-client.rules
include $RULE_PATH/community-web-dos.rules
include $RULE_PATH/community-web-iis.rules
include $RULE_PATH/community-web-misc.rules
include $RULE_PATH/community-web-php.rules
include $RULE_PATH/custom.rules
Step #8: Customize your preprocessor and decoder alerts
For more information, see README.decoder_preproc_rules
decoder and preprocessor event rules
include $PREPROC_RULE_PATH/preprocessor.rules
include $PREPROC_RULE_PATH/decoder.rules
include $PREPROC_RULE_PATH/sensitive-data.rules
^G Get Help ^O WriteOut ^R Read File ^Y Prev Page ^K Cut Text ^C Cur Pos
^X Exit ^J Justify ^W Where Is ^V Next Page ^U UnCut Text ^T To Spell
Right Ctrl


server1 [Running] - Oracle VM VirtualBox
Machine View Devices Help
root@ubuntu:~# snort -l ./log -b -c /etc/snort/snort.conf -r data.pcap
Right Ctrl


server1 [Running] - Oracle VM VirtualBox
Machine View Devices Help
root@ubuntu:~# cd log/
root@ubuntu:~/log# ls
alert snort.log.1488978066
root@ubuntu:~/log#
Right Ctrl





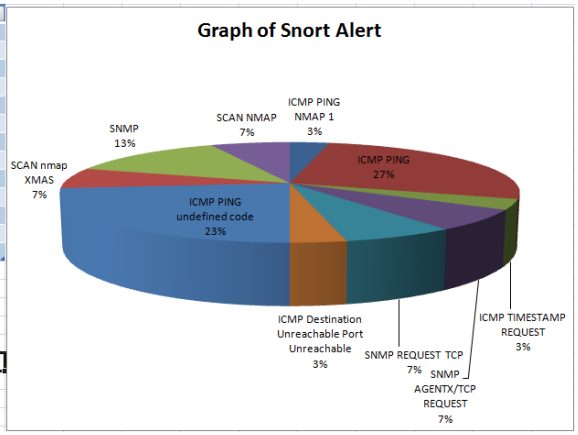

```
[**] [1:469:3] ICMP PING NMAP [**]
[Classification: Attempted Information Leak] [Priority: 2]
03/08-19:20:01.564735 10.0.2.15 -> 104.16.213.202
ICMP TTL:49 TOS:0x0 ID:16825 IpLen:20 DgmLen:28
Type:8  Code:0  ID:58299   Seq:0  ECHO
[Xref => http://www.whitehats.com/info/IDS162]

[**] [1:384:5] ICMP PING [**]
[Classification: Misc activity] [Priority: 3]
03/08-19:20:01.564735 10.0.2.15 -> 104.16.213.202
ICMP TTL:49 TOS:0x0 ID:16825 IpLen:20 DgmLen:28
Type:8  Code:0  ID:58299   Seq:0  ECHO

[**] [1:453:5] ICMP Timestamp Request [**]
[Classification: Misc activity] [Priority: 3]
03/08-19:20:01.565050 10.0.2.15 -> 104.16.213.202
ICMP TTL:53 TOS:0x0 ID:59645 IpLen:20 DgmLen:40
Type:13  Code:0  ID: 21508  Seq: 0  TIMESTAMP REQUEST

[**] [1:1421:11] SNMP AgentX/tcp request [**]
[Classification: Attempted Information Leak] [Priority: 2]
03/08-19:20:16.326556 10.0.2.15:47523 -> 104.16.213.202:705
TCP TTL:37 TOS:0x0 ID:45870 IpLen:20 DgmLen:44
******S* Seq: 0xDF0566CA  Ack: 0x0  Win: 0x400  TcpLen: 24
TCP Options (1) => MSS: 1460
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=
2002-0013][Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?
name=2002-0012][Xref => http://www.securityfocus.com/bid/4132]
[Xref => http://www.securityfocus.com/bid/4089][Xref =>
http://www.securityfocus.com/bid/4088]
```

	Column1	Column2
4	ICMP PING NMAP 1	1
5	ICMP PING	8
6	ICMP TIMESTAMP REQUEST	1
7	SNMP AGENTX/TCP REQUEST	2
8	SNMP REQUEST TCP	2
9	ICMP Destination Unreachable Port Unreachable	1
10	ICMP PING undefined code	7
11	SCAN nmap XMAS	2
12	SNMP	4
13	SCAN NMAP	2



ANALISIS:

Telah diperhatikan bahwa setiap alert terbagi dalam masing-masing kelompok dan tersusun dengan rapi sesuai dengan urutan data yang didapatkan. Data yang disajikan adalah data hasil segmentasi dari aplikasi wireshark terhadap penggunaan nmap untuk target. Hal ini akan menghasilkan beberapa titik-titik penyerangan untuk bahan analisis.

Perlu diketahui peggunaan rules oleh penulis tidaklah semua rules digunakan dan juga proses scanning yang dilakukan tidaklah lama untuk mendapatkan banyak informasi, hal ini mengakibatkan data yang didapatkan tidaklah maksimal. Namun untuk penggunaan awal dari aplikasi snort diharapkan sudah sesuai dengan kebutuhan dan perlu untuk dikembangkan lagi.